



*ZW*  
*AF*  
*2134*

THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Peyravian

Serial No.: 09/459,187

Filed: December 10, 1999

For: **TIME STAMPING METHOD USING TIME IN  
TSA'S PUBLIC KEY CERTIFICATE**

Attorney's Docket No: 4541-006

Examiner: Simitoski, Michael J

Group Art Unit: 2134

Confirmation No.: 9759

Mail Stop Appeal Brief - Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**CERTIFICATE OF MAILING**

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on March 11, 2005.

*Kathleen Koppen*  
Kathleen Koppen

**APPEAL BRIEF**

This Appeal Brief is being submitted in triplicate not more than two months after the Office received the Notice of Appeal (January 18, 2005). As such, no extension of time fees should be due. The Commissioner is authorized to charge the requisite fee pursuant to 37 C.F.R. §41.20 and any additional fees required to IBM's Deposit Account No. 09/0461.

**(1) REAL PARTY IN INTEREST**

The real party in interest is IBM Corporation, assignee of the present invention.

**(2) RELATED APPEALS AND INTERFERENCES**

There are no related appeals or interferences to the best of Applicant's knowledge.

### **(3) STATUS OF CLAIMS**

Claims 1-11 were originally filed with the application, and claim 12 was added in a preliminary amendment filed concurrently with a Request for Continued Examination (RCE). Claims 1-12 are therefore currently pending and stand rejected. Accordingly, Applicant appeals the rejection of claims 1-12.

### **(4) STATUS OF AMENDMENTS**

All amendments have been entered to the best of Applicant's knowledge.

### **(5) SUMMARY OF CLAIMED SUBJECT MATTER**

Independent claim 1 relates to a method of time-stamping digital documents so that the date of the document may later be verified. The method relies on the services of a trusted agent, referred to herein as the Time Stamping Authority (TSA). *Spec.*, pg. 4, ll. 13-17.

According to the embodiment of claim 1, the TSA receives identifying data associated with a document that is created by the document author. For example, the identifying data may be a hash value of the document or a portion thereof. *Spec.*, pg. 5, ln. 10 – pg. 6, ln. 19. The TSA also has a time-based private signature key that it uses to sign time stamp receipts. *Spec.*, pg. 6, ll. 19-20. The private signature key is associated with a fixed time reference. *Spec.*, pg. 7, ll. 3-8. Upon receipt of the identifying data, the TSA computes a time difference between the fixed time reference associated with the private signature key and the current time as generated by a trusted clock controlled by the TSA or some other trusted source. *Spec.*, pg. 7, ll. 9-12. The computed time difference is then appended to the identifying data received by the TSA to create the time-stamp receipt and certified by the TSA before transmittal to the requesting author. *Spec.*, pg. 7, ll. 13-23.

Should a dispute arise as to the document's authenticity, the time-stamp receipt is verified using the TSA's public verification key. The public verification key also includes the

fixed time reference associated with the private signature key. The hash value in the time stamp receipt is then compared to a hash value generated for the disputed copy of the document. The time difference included in the time-stamped receipt is then added to the fixed time reference included in the public verification key. If this information is the same, the existence and substance of the document as of a particular date is proven. *Spec.*, pg. 7, ln. 24 – pg. 8, ln. 9.

## **(6) GROUNDS OF REJECTION**

The Examiner rejected claims 1-12 under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,136,647 to Haber (hereinafter “Haber”).

## **(7) ARGUMENTS RELATING TO THE §102 GROUND OF REJECTION**

### **A. The patent to Haber fails to anticipate any of claims 1-12**

Claim 1 is directed to a method of time-stamping a document that may be used to later verify the document. For reference, claim 1 appears below.

1. A method for time stamping a document comprising:
  - receiving identifying data associated with said document at an outside agency;
  - computing at said outside agency a time difference between a predetermined time reference and the time of receipt of said identifying data;
  - creating a time stamp receipt by associating said time difference with said identifying data; and
  - certifying said time stamp receipt by signing said time stamp receipt at said outside agency with a private signature key associated with said predetermined time reference.

The method of claim 1 recites that the outside agency (e.g., the TSA) computes a time difference between a predetermined time reference and the time the outside agency received the identifying data from a requestor. These two times are completely different time values, and thus, claim 1 requires computing the time difference as a delta between two completely different time values. In contrast to the Examiner's assertion, Haber fails to teach this computation.

Haber discloses a method of time-stamping a document by a trusted outside agency. Unlike the invention of claim 1, however, Haber never teaches computing the requisite time difference. This is because Haber uses a different method to generate the time-stamp receipt altogether. Specifically, Haber concatenates a plurality of current times in a chronological sequence for inclusion into the time-stamp receipt. These current times are actual system times that reflect the receipt times of documents at the outside agency.

For each given processed document  $D_k$ , the TSA generates a time-stamp receipt which includes, for example, a sequential receipt number,  $r_k$ , the identity of the author,  $A_k$ , by ID number  $ID_k$ , or the like, the hash,  $H_k$ , of the document, and the current time,  $t_k$ . In addition, the TSA includes the receipt data of the immediately preceding processed document,  $D_{k-1}$ , of author,  $A_{k-1}$ , thereby bounding the timestamp of document,  $D_k$ , in the "past" direction by the independently established earlier receipt time,  $t_{k-1}$ . Likewise, the receipt data of the next received document,  $D_{k+1}$ , are included to bound the time-stamp of document,  $D_k$ , in the "future" direction. The composite receipt, now containing the time data of the three, or more if desired, sequential time-stamp receipts, or identifying segments thereof, is then certified with the cryptographic TSA signature and transmitted to the author,  $A_k$ .

*Haber*, col. 4, ll. 6-24 (emphasis added). As evidenced by the above passage,  $t_{k+1}$ , and  $t_{k-1}$  define actual time of receipt values for documents received both before and after the document currently being time-stamped. Each time value is independently established and bounds the current receipt time  $t_k$  of the document being time-stamped in a continuum of time (i.e., in the "past" and in the "future").

The chronological sequence of Haber is not the requisite computed time difference, and Haber never asserts that it is. Haber does not disclose that the TSA computes a difference between any of these times, let alone between a current time and a predetermined reference time. In an attempt to explain this deficiency, the Examiner rests on the theory that the current times in Haber are computer times reflecting the number of elapsed milliseconds from a reference time (e.g., January 1, 1970 for UNIX systems). However, this assertion simply fails scrutiny because it fails to address the elements of claim 1. Particularly, claim 1 requires computing the difference between two different values and including the time difference in the

time-stamp receipt. At best, the Examiner's assertion means only that Haber could be construed to teach how the two separate time values of claim 1 (i.e., the predetermined time reference and the current time of receipt) are obtained. It cannot, however, be construed to teach computing the difference between those two values.

Simply put, Haber fails to teach the "computing limitation of claim 1, and indeed, this is not surprising. According to Haber, fixing the time-stamp in a continuum of time is so effective that it could render the signing the time-stamp receipt with the TSA's private signature key "superfluous in actual practice." *Haber*, col. 4, ll. 25-33. Thus, not only does Haber not compute the time difference as required by claim 1, but also, Haber never appears to even contemplate doing so. Because Haber fails to disclose the requisite "computing" element of claim 1, it necessarily fails to anticipate claim 1 under §102 as a matter of law.

In addition, however, Haber fails to teach the "creating" and "certifying" elements of claim 1. Both elements explicitly recite the use of the computed time difference that Haber fails to teach in performing these steps. However, Haber creates a time-stamp receipt by concatenating a sequence of received times values. It is this chronological sequence that is certified by the outside agency with a private key, not a computed time difference.

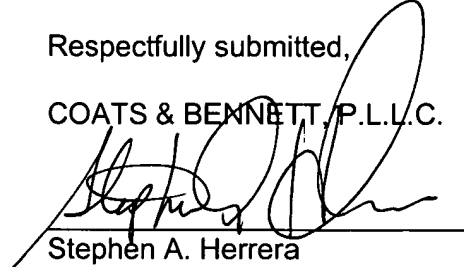
Anticipation under 35 U.S.C. §102 requires that a single prior art reference disclose every element or limitation exactly as claimed. *In re Bond*, 910 F.2d 831, 323 (Fed. Cir. 1990). The patent to Haber simply fails to meet this legal standard. Accordingly, the §102 rejection leveled by the Examiner must fail.

**Conclusion**

For the reasons set forth above, Applicant submits that the Examiner has failed to establish that the reference to Haber anticipates the pending claims as required under the law, and thus, all claims being appealed herein are patentable over the cited art.

Respectfully submitted,

COATS & BENNETT, P.L.L.C.

A handwritten signature in black ink, appearing to read "Stephen A. Herrera", is written over a horizontal line. The signature is stylized with large, flowing loops.

Stephen A. Herrera  
Registration No.: 47,642  
Telephone: (919) 854-1844

Dated: March 11, 2005

**(8) CLAIMS APPENDIX**

1. A method for time stamping a document comprising:
  - receiving identifying data associated with said document at an outside agency;
  - computing at said outside agency a time difference between a predetermined time reference and the time of receipt of said identifying data;
  - creating a time stamp receipt by associating said time difference with said identifying data; and
  - certifying said time stamp receipt by signing said time stamp receipt at said outside agency with a private signature key associated with said predetermined time reference.
2. The time stamping method of claim 1 further including transmitting said certified time stamp receipt to a designated party.
3. The time stamping method of claim 1 wherein said identifying data comprises a digital copy of at least a portion of said document.
4. The time stamping method of claim 3 wherein said identifying data comprises a digital representation of said document derived by application of a deterministic function to at least a portion of said document.
5. The time stamping method of claim 4 wherein said digital representation is a hash value derived by application of a one-way hashing function to at least a portion of said document.

6. The time stamping method of claim 1 wherein said time stamp receipt includes a copy of at least a portion of said identifying data concatenated with said time difference.

7. The time stamping method of claim 6 wherein said time stamp receipt includes a digital sequence derived from said identifying data concatenated with said time difference.

8. The time stamping method of claim 1 wherein said time stamp receipt further includes an identification number associated with the document originator.

9. The time stamping method of claim 8 wherein said time stamp receipt further includes a sequential record number.

10. The time stamping method of claim 1 wherein said time reference is stored in a public key certificate.

11. The time stamping method of claim 1 wherein the step of certifying said time stamp receipt includes encrypting said time stamp receipt using a private signature key controlled by said outside agency, wherein said time stamp receipt can be later verified by decrypting the signed time stamp receipt with a corresponding public verification key.



12. A method for time stamping a document comprising:

receiving identifying data associated with said document at an outside agency;  
determining the time of receipt of said identifying data at said outside agency;  
computing at said outside agency a time difference between a predetermined time reference  
and said time of receipt;  
associating said time difference with said identifying data to create a time stamp receipt; and  
certifying said time stamp receipt by signing said time stamp receipt at said outside agency  
with a private signature key associated with said predetermined time reference.

**(9) EVIDENCE APPENDIX**

There is no further evidence not contained in the prosecution history.

**(10) RELATED PROCEEDINGS APPENDIX**

There are no related proceedings.